TRANSPARENCY RECORD

Public Service Commission Te Kawa Mataaho

Absence of Risk Assessment on Physical Coercion, Kidnapping and Duress Scenarios involving Digital ID

OIA 2026-0218 | Response dated 4 August 2026

1. Purpose of this Record

This document records the formal Official Information Act response from the Public Service Commission Te Kawa Mataaho to a request concerning risk assessments, contingency planning, and analysis of physical coercion, kidnapping, forced disclosure, and duress scenarios involving Digital ID credentials and linked services.

It is published as a primary-source transparency record. It sits alongside the independent Digital ID Physical Coercion Risk Briefing (July 2026) and other formal admissions that specific categories of risk analysis do not exist.

2. The Request

The request, received by the Public Service Commission on 13 July 2026, sought:

1. Any specific risk assessments regarding physical coercion, kidnapping, forced disclosure, or duress scenarios involving Digital ID credentials or linked services.
2. Any analysis of emerging crime trends involving digital assets (such as cryptocurrency-related kidnappings, home invasions, and extortion) and their implications for Digital ID systems and single sign-on architectures.
3. Any contingency planning, mitigation measures, or fallback processes for situations where an individual is physically compelled to authenticate, transfer access, or disclose information via Digital ID.
4. Any analysis of the concentration of risk if Digital ID becomes a central or master key to multiple government and commercial services (banking, benefits, property, travel, healthcare, work authorisation, etc.).
5. Any internal advice, reports, or briefings addressing the human-factor / physical compromise vulnerabilities of Digital ID systems, as opposed to purely technical or cybersecurity risks.

3. The Commission’s Formal Response

Key statements:

- The scenarios outlined in the request “have not been assessed as materially different from similar risks that can arise with current forms of identification or other personal information.”
- “On that basis, no separate risk assessment or analysis has been prepared specifically for Digital ID credentials in relation to those scenarios.”
- Issuers who provide digital ID credentials “may consider this as part of the development of their services.”

Formal refusal under section 18(e)

The entire request was refused under section 18(e) of the Official Information Act 1982:

> *“I am therefore refusing your request in full under section 18(e) of the OIA on the grounds the information requested does not exist.”*

This refusal covers all five parts of the request: specific risk assessments of physical coercion and related scenarios; analysis of emerging digital-asset crime trends; contingency planning or fallback processes for physical compulsion; analysis of

concentration of risk if Digital ID becomes a master key; and internal advice on human-factor / physical compromise vulnerabilities.

4. What This Record Establishes

This response establishes, in writing from the Public Service Commission:

- That the physical coercion, kidnapping, forced disclosure and duress scenarios described have not been assessed as materially different from risks already associated with existing forms of identification.
- That no separate risk assessment or analysis has been prepared specifically for Digital ID credentials in relation to those scenarios.
- That no contingency planning, mitigation measures or fallback processes specific to physical compulsion involving Digital ID have been identified as existing.
- That no analysis of concentration of risk arising from Digital ID as a potential master key to multiple services has been located.
- That no internal advice, reports or briefings addressing human-factor / physical compromise vulnerabilities of Digital ID systems (as distinct from technical cybersecurity risks) have been located.

5. Context

Digital identity systems are being developed and promoted as a means of streamlining access to government and commercial services. As such systems become more central, questions arise about the concentration of risk if a single credential or authentication pathway becomes a master key to banking, benefits, property, travel, healthcare and other critical services.

Parallel to this, crime trends involving digital assets (including cryptocurrency-related kidnappings, home invasions and extortion) have been reported internationally. These raise the possibility of physical coercion directed at an individual’s ability to authenticate or transfer access.

This formal response from the Public Service Commission confirms that no dedicated risk assessment, contingency planning or analysis of these human-factor / physical compromise scenarios has been prepared specifically for Digital ID. The Commission’s position is that the scenarios are not materially different from risks already present with existing forms of identification.

6. What This Record Does Not Establish

- That Digital ID systems are inherently unsafe or should not proceed.
- That issuers of Digital ID credentials have failed to consider physical compromise risks (the Commission notes they may do so as part of service development).
- That the information must exist elsewhere and is being withheld. The Commission has stated that it does not exist.

7. Public Interest

Where the Public Service Commission confirms that no separate risk assessment or analysis has been prepared specifically for Digital ID in relation to physical coercion, kidnapping, duress, contingency planning for physical compulsion, or concentration of risk as a master key, that confirmation is itself a matter of public interest.

This record is published so that the Commission’s formal statement sits on the public record alongside the independent Digital ID Physical Coercion Risk Briefing and the wider pattern of formal admissions that certain categories of risk analysis do not exist.

8. Source Document

Letter from Nicky Dirks, Manager – Ministerial and Executive Services, Public Service Commission Te Kawa Mataaho, dated 4 August 2026, responding to Official Information Act request OIA 2026-0218.

Related records: Digital ID Physical Coercion Risk Briefing (July 2026); other formal "does not exist" responses on infrastructure analysis, co-governance accountability analysis, and comparative managed retreat assessments (2026).

— End of Record —

Independent researcher | Public interest documentation | August 2026